

RATIONALITY CONDITIONS FOR THE EIGENVALUES OF NORMAL FINITE CAYLEY GRAPHS

CHRIS GODSIL AND PABLO SPIGA

ABSTRACT. Given a finite group G , we say that a subset C of G is power-closed if, for every $x \in C$ and $y \in \langle x \rangle$ with $\langle x \rangle = \langle y \rangle$, we have $y \in C$.

In this paper we are interested in finite Cayley digraphs $\text{Cay}(G, C)$ over G with connection set C , where C is a union of conjugacy classes of G . We show that each eigenvalue of $\text{Cay}(G, C)$ is integral if and only if C is power-closed. This result will follow from a discussion of some more general rationality conditions on the eigenvalues of $\text{Cay}(G, C)$.

1. INTRODUCTION

Let G be a finite group and let C be a subset of G . The *Cayley digraph* $\text{Cay}(G, C)$ over G with connection set S is the digraph with vertex set G and with (g, h) being a directed arc if and only if $gh^{-1} \in C$. The *eigenvalues* of a digraph are the eigenvalues of its adjacency matrix.

In this paper we are concerned with some rationality conditions on the eigenvalues of $\text{Cay}(G, C)$ when C is a union of G -conjugacy classes. (Cayley digraphs of this form are sometimes called *normal*.) In particular, we are interested in the case that each eigenvalue of $\text{Cay}(G, C)$ is rational. Observe that since the eigenvalues of a digraph are algebraic integers (being the zeros of the characteristic polynomial of a matrix with integer coefficients), we see that if λ is a rational eigenvalue of $\text{Cay}(G, C)$, then λ is actually an integer.

We say that $C \subseteq G$ is *power-closed* if, for every $x \in C$ and $y \in \langle x \rangle$ with $\langle y \rangle = \langle x \rangle$, we have $y \in C$.

Theorem 1.1. *Let G be a finite group and let C be a union of conjugacy classes of G . Then each eigenvalue of $\text{Cay}(G, C)$ is an integer if and only if C is power-closed.*

As every power-closed subset C is inverse-closed (that is, $C = C^{-1}$), it follows that if each eigenvalue of $\text{Cay}(G, C)$ is an integer, then $\text{Cay}(G, C)$ is an undirected graph. Theorem 1.1 gives a rather efficient (and linear-algebra-free) test to check when a Cayley digraph has only integer eigenvalues.

We note that, aside from its inherent interest, there are other reasons to consider this question. Let X be a graph on n vertices with adjacency matrix A . A *continuous quantum walk* of graph is specified by the family of matrices

$$U(t) := \exp(itA), \quad (t \in \mathbb{R}).$$

If $u \in V(X)$ we use e_u to denote the standard basis vector in \mathbb{R}^n indexed by u . We say that X is *periodic* at u if there is a complex scalar γ of norm 1 and a positive

2000 *Mathematics Subject Classification.* 05C50, 20C15.

Key words and phrases. conjugacy classes, eigenvalues, irreducible characters.

Address correspondence to P. Spiga, E-mail: pablo.spiga@unimib.it.

time t such that

$$U(t)e_a = \gamma e_a.$$

For surveys on this topic see, e.g., [5, 6]. In [7] Saxena, Severini and Shparlinski showed that if X was a circulant, then X was periodic at a vertex if and only if the eigenvalues of X were integers. Subsequently it was shown in [4] that this conclusion held for any vertex-transitive graph, not just for circulants. This work has motivated the search for nice classes of vertex-transitive graphs with integer eigenvalues.

For abelian groups, our theorem is a well-known and classical result of Bridges and Mena [2, Theorem 2.4] (observe that for an abelian group G , every subset of G is a union of G -conjugacy classes). In particular, Theorem 1.1 generalizes the work of Bridges and Mena by dropping the hypothesis of G being abelian and by replacing it with a natural condition on the connection set.

Theorem 1.1 will follow at once from a slightly more general theorem. Before giving its statement we need some preliminary notation, which we will use throughout the whole paper, and some observations. Here we follow closely [8].

Let G be a finite group and let C be a union of conjugacy classes of G . From [1] or [3], we get that the eigenvalues of $\text{Cay}(G, C)$ are

$$(1) \quad \frac{1}{\chi(1)} \sum_{x \in C} \chi(x),$$

as χ runs through the set of irreducible complex characters of G . (We denote this set by $\text{Irr}_{\mathbb{C}}(G)$.)

Following Serre [8, Section 9.1], we denote by $R_{\mathbb{C}}(G)$ the subring of the class functions of G generated by $\text{Irr}_{\mathbb{C}}(G)$, that is,

$$R_{\mathbb{C}}(G) = \bigoplus_{\chi \in \text{Irr}_{\mathbb{C}}(G)} \mathbb{Z}\chi.$$

More generally, given a field K with $\mathbb{Q} \leq K \leq \mathbb{C}$, we denote by $R_K(G)$ the subring of $R_{\mathbb{C}}(G)$ generated by the characters of the representations of G over K .

We let m be the least common multiple of the order of the elements of G , $\mathbb{Q}(m)$ the algebraic field obtained by adjoining the m th roots of unity to \mathbb{Q} and $\Gamma_{\mathbb{Q}}$ the Galois group of $\mathbb{Q}(m)$ over \mathbb{Q} . By a well-known theorem of Brauer [8, Theorem 24], we have $R_{\mathbb{C}}(G) = R_{\mathbb{Q}(m)}(G)$, that is, every complex irreducible representation of G is realizable over $\mathbb{Q}(m)$. In particular, every $\chi \in \text{Irr}_{\mathbb{C}}(G)$ has values in $\mathbb{Q}(m)$ and hence, from (1), every normal Cayley digraph $\text{Cay}(G, C)$ has all of its eigenvalues in $\mathbb{Q}(m)$.

Now, let ε be a primitive m th root of unity. From a celebrated theorem of Gauss, the m th cyclotomic polynomial is irreducible over \mathbb{Q} and hence $\Gamma_{\mathbb{Q}} \cong (\mathbb{Z}/m\mathbb{Z})^*$ (where $(\mathbb{Z}/m\mathbb{Z})^*$ denotes the invertible elements of the ring $\mathbb{Z}/m\mathbb{Z}$). Here we identify $\Gamma_{\mathbb{Q}}$ with $(\mathbb{Z}/m\mathbb{Z})^*$ under this isomorphism. More precisely, for $\sigma \in \Gamma_{\mathbb{Q}}$, there exists a unique $t \in (\mathbb{Z}/m\mathbb{Z})^*$ with $\sigma(\varepsilon) = \varepsilon^t$.

Finally, given a field K with $\mathbb{Q} \leq K \leq \mathbb{Q}(m)$, we denote by Γ_K the image of $\text{Gal}(\mathbb{Q}(m)/K)$ in $(\mathbb{Z}/m\mathbb{Z})^*$, and if $t \in \Gamma_K$, we let σ_t denote the corresponding element of $\text{Gal}(\mathbb{Q}(m)/K)$.

For $s \in G$ and for an integer n , the element $s^n \in G$ depends only on the residue class of n modulo the order of s , and hence only on n modulo m . Therefore, s^t is

defined for each $t \in \Gamma_K$, and the group Γ_K induces an action on the underlying set of G .

Definition 1.2. We say that $g, h \in G$ are Γ_K -conjugate, if there exists $t \in \Gamma_K$ such that g and h^t are conjugate in G . Clearly, being Γ_K -conjugate is an equivalence relation in G , and we call Γ_K -conjugacy classes its equivalence classes.

Observe that when $K = \mathbb{Q}(m)$, we have $\Gamma_K = 1$ and hence the Γ_K -conjugacy classes coincide with the G -conjugacy classes. Moreover, when $K = \mathbb{Q}$, we have $\Gamma_K = (\mathbb{Z}/m\mathbb{Z})^*$ and hence two elements g and h of G are Γ_K -conjugate if there exists $t \in (\mathbb{Z}/m\mathbb{Z})^*$ with g conjugate to h^t in G .

We are finally ready to state the main result of this paper.

Theorem 1.3. *Let G be a finite group, let C be a union of G -conjugacy classes, let m be the least common multiple of the order of the elements of G and let K be a field with $\mathbb{Q} \leq K \leq \mathbb{Q}(m)$. Then each eigenvalue of $\text{Cay}(G, C)$ lies in K if and only if C is a union of Γ_K -conjugacy classes.*

2. PROOFS

Theorem 1.1 follows from Theorem 1.3 (applied with $K = \mathbb{Q}$) and the following lemma.

Lemma 2.1. *Let G be a finite group and let C be a union of G -conjugacy classes. Then C is power-closed if and only if C is a union of $\Gamma_{\mathbb{Q}}$ -conjugacy classes.*

Proof. We first suppose that C is power-closed and we show that C is a union of $\Gamma_{\mathbb{Q}}$ -conjugacy classes. Let $x \in C$ and let $y \in G$ be $\Gamma_{\mathbb{Q}}$ -conjugate to x . Then, by definition, there exists $t \in (\mathbb{Z}/m\mathbb{Z})^*$ with y^t conjugate to x in G , that is, $y^t = x^g$ for some $g \in G$. Now, $x^g \in C$ and $\langle y \rangle = \langle y^t \rangle = \langle x^g \rangle$, thus $y \in C$ because C is power-closed.

Conversely, we suppose that C is a union of $\Gamma_{\mathbb{Q}}$ -conjugacy classes and we show that C is power-closed. Let $x \in C$ and $y \in \langle x \rangle$ with $\langle y \rangle = \langle x \rangle$. Then $y = x^{t'}$, for some integer t' coprime to the order $|x|$ of x . From Dirichlet's theorem on primes in arithmetic progression, there exists a prime $t \in \{t' + \ell|x| \mid \ell \in \mathbb{Z}\}$ with $t > m$. We get that the residue class of t in $\mathbb{Z}/m\mathbb{Z}$ is invertible. Now $x^t = x^{t'} = y$ and hence x and y are $\Gamma_{\mathbb{Q}}$ -conjugate. Thus $y \in C$. \square

Proof of Theorem 1.3. Suppose that C is a union $C_1 \cup \dots \cup C_\ell$ of Γ_K -conjugacy classes. From (1), we need to show that $\sum_{x \in C} \chi(x)/\chi(1) \in K$, for every $\chi \in \text{Irr}_{\mathbb{C}}(G)$. For simplicity, we write $e_\chi = \sum_{x \in C} \chi(x)/\chi(1)$. As

$$e_\chi = \frac{1}{\chi(1)} \sum_{x \in C} \chi(x) = \left(\frac{1}{\chi(1)} \sum_{x \in C_1} \chi(x) \right) + \dots + \left(\frac{1}{\chi(1)} \sum_{x \in C_\ell} \chi(x) \right),$$

it suffices to consider the case that $C = C_1$ is a Γ_K -conjugacy class. In particular, from the definition of Γ_K -conjugacy class we get $C = (x^{t_0})^G \cup \dots \cup (x^{t_\ell})^G$, for some $x \in G$ and some $t_0, \dots, t_\ell \in \Gamma_K$. (We denote by x^G the conjugacy class of x under G .) Observe that the action of the group Γ_K on C induces a transitive action of Γ_K on $\{(x^{t_0})^G, \dots, (x^{t_\ell})^G\}$.

Fix $\chi \in \text{Irr}_{\mathbb{C}}(G)$ and let ρ be a representation of G affording the character χ . Let $t \in \Gamma_K$ and let σ be the corresponding element in $\text{Gal}(\mathbb{Q}(m)/K)$. For $s \in G$, let $\omega_1, \dots, \omega_{\chi(1)}$ be the eigenvalues of $\rho(s)$. As $|s|$ is a divisor of m , we get that

ω_i is an m th root of unity and hence the eigenvalues of $\rho(s^t)$ are the $\omega_1^t, \dots, \omega_{\chi(1)}^t$. Thus we have

$$(2) \quad (\chi(s))^\sigma = \left(\sum_{i=1}^{\chi(1)} \omega_i \right)^\sigma = \sum_{i=1}^{\chi(1)} \omega_i^t = \chi(s^t).$$

Now applying σ to e_χ , using (2) and recalling that the set C is invariant under taking t th powers, we get $e_\chi^\sigma = e_\chi$. In particular, $e_\chi^\sigma = e_\chi$ for every $\sigma \in \text{Gal}(\mathbb{Q}(m)/K)$. Since $\mathbb{Q}(m)/K$ is a Galois extension, we have $e_\chi \in K$.

Conversely, suppose that each eigenvalue of $\text{Cay}(G, C)$ lies in K . Since C is a union of G -conjugacy classes, for showing that C is also a union of Γ_K -conjugacy classes it suffices to prove that, for each $x \in C$ and for each $t \in \Gamma_K$, we have $x^t \in C$. We argue by induction on $|x|$. Clearly, if $|x| = 1$, then there is nothing to prove. Now assume that $|x| > 1$. Let $\eta \in \mathbb{C}$ be a primitive $|x|$ th root of unity, let $\theta : \langle x \rangle \rightarrow \mathbb{C}$ be the irreducible character of $\langle x \rangle$ with $\theta(x) = \eta$, and let $\Theta = \text{Ind}_{\langle x \rangle}^G(\theta)$, that is, Θ is the character of G obtained by inducing θ from $\langle x \rangle$ to G . From [8, page 55], we have

$$(3) \quad \Theta(s) = \frac{1}{|x|} \sum_{\substack{y \in G \\ y^{-1}sy \in \langle x \rangle}} \theta(y^{-1}sy).$$

Since Θ is a character of G , Θ is an integral linear combination of the irreducible characters of G . Moreover, since every eigenvalue of $\text{Cay}(G, C)$ lies in K , from (1) we obtain $\sum_{z \in C} \Theta(z) \in K$. Write $e_\Theta := |x| \sum_{z \in C} \Theta(z)$. From (3), we get

$$\begin{aligned} e_\Theta &= \sum_{z \in C} \sum_{\substack{y \in G \\ y^{-1}zy \in \langle x \rangle}} \theta(y^{-1}zy) = \sum_{z \in C} \sum_{i=0}^{|x|-1} \sum_{\substack{y \in G \\ y^{-1}zy = x^i}} \theta(x^i) = \sum_{z \in C} \sum_{i=0}^{|x|-1} \sum_{\substack{y \in G \\ y^{-1}zy = x^i}} \eta^i \\ (4) \quad &= \sum_{i=0}^{|x|-1} \sum_{z \in C} \sum_{\substack{y \in G \\ y^{-1}zy = x^i}} \eta^i = a_0 \eta^0 + a_1 \eta^1 + \dots + a_{|x|-1} \eta^{|x|-1}, \end{aligned}$$

where $a_0, \dots, a_{|x|-1}$ are non-negative integers. More precisely,

$$(5) \quad a_i = |\{(z, y) \mid z \in C, y \in G, y^{-1}zy = x^i\}|.$$

Furthermore, $a_1 > 0$ because $x \in C$.

Now, let $t \in \Gamma_K$ and let σ be its corresponding element in $\text{Gal}(\mathbb{Q}(m)/K)$. Applying σ on both sides of (4) we get

$$e_\Theta = e_\Theta^\sigma = a_0 \eta^0 + a_1 \eta^t + a_2 \eta^{2t} + \dots + a_{|x|-1} \eta^{(|x|-1)t}$$

and hence

$$(6) \quad (a_0 - a_0) \eta^0 + (a_1 - a_{t-1}) \eta^1 + (a_2 - a_{2t-1}) \eta^2 + \dots + (a_{|x|-1} - a_{(|x|-1)t-1}) \eta^{|x|-1} = 0,$$

where the indices are computed modulo $|x|$. Now, observe that from our induction hypothesis, for every divisor i of $|x|$ with $1 < i < |x|$, the elements x^i and x^{it} are either both in C or both in $G \setminus C$. In the first case, from (5), we have $a_i = a_{it}$. In the second case, $a_i = 0$ and $a_{it} = 0$ and hence again $a_i = a_{it}$. It follows that the

only summands in (6) that are possibly not zero correspond to the primitive $|x|$ th roots of unity. Therefore (6) gives rise to the linear equation

$$\sum_{\substack{i=0 \\ \text{Gcd}(i, |x|)=1}}^{|x|-1} (a_i - a_{i+1}) \eta^i = 0.$$

From a celebrated theorem of Gauss, $(\eta^i \mid 0 \leq i \leq |x| - 1, \text{Gcd}(i, |x|) = 1)$ is a basis for $\mathbb{Q}(\eta)$ over \mathbb{Q} and hence $a_i = a_{i+1}$, for every i . In particular, $a_t = a_1 > 0$ and hence $x^t \in C$ from (5). \square

REFERENCES

- [1] L. Babai, Spectra of Cayley Graphs, *J. Combin. Theory B.* **2**, (1979), 180–189.
- [2] W. G. Bridges, R. A. Mena, Rational G -matrices with rational eigenvalues, *J. Combin. Theory Ser. A* **32**, (1982).
- [3] P. Diaconis, M. Shahshahani, Generating a Random Permutation with Random Transpositions, *Zeit. für Wahrscheinlichkeitstheorie* **57** (1981), 159–179.
- [4] C. Godsil, Periodic Graphs, *Electronic J. Combinatorics* **18**(1):\#23, June 2011.
- [5] C. Godsil, State transfer on graphs, *Discrete Math.* **312** (2012), 129–147.
- [6] J. Kempe, Quantum random walks - an introductory overview, *Contemporary Physics* **44** (2003), 307–327. arxiv:0303081.
- [7] N. Saxena, S. Severini, I. Shparlinski, Parameters of integral circulant graphs and periodic quantum dynamics, *International Journal on Quantum Computation* **5**(3) (2007), 417–430. arXiv:quant-ph/0703236.
- [8] J-P. Serre, Linear Representations of Finite Groups, Graduate Texts in Mathematics **42**, Springer-Verlag, 1977.

CHRIS GODSIL, DEPARTMENT OF COMBINATORICS AND OPTIMIZATION, UNIVERSITY OF WATERLOO, CANADA
E-mail address: cgodsil@math.uwaterloo.ca

PABLO SPIGA, DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITY OF MILANO-BICOCCA, ITALY
E-mail address: pablo.spiga@unimib.it